PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04B — A2

(11) International Publication Number: WO 99/33188

(43) International Publication Date: 1 July 1999 (01.07.99)

(21) International Application Number: PCT/US98/25961

(22) International Filing Date: 8 December 1998 (08.12.98)

(30) Priority Data:
08/997,692 — 23 December 1997 (23.12.97) — US

(71) Applicant: BRIGHT LIGHT TECHNOLOGIES, INC. [US/US]; Suite 300, 651 Brannan Street, San Francisco, CA 94107 (US).

(72) Inventor: PAUL, Sunil; 1506 Willard Street, San Francisco, CA 94117 (US).

(74) Agent: LUEDKE, Adriana, Suringa; Covington & Burling, 1201 Pennsylvania Avenue, N.W., P.O. Box 7566, Washington, DC 20044-7566 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

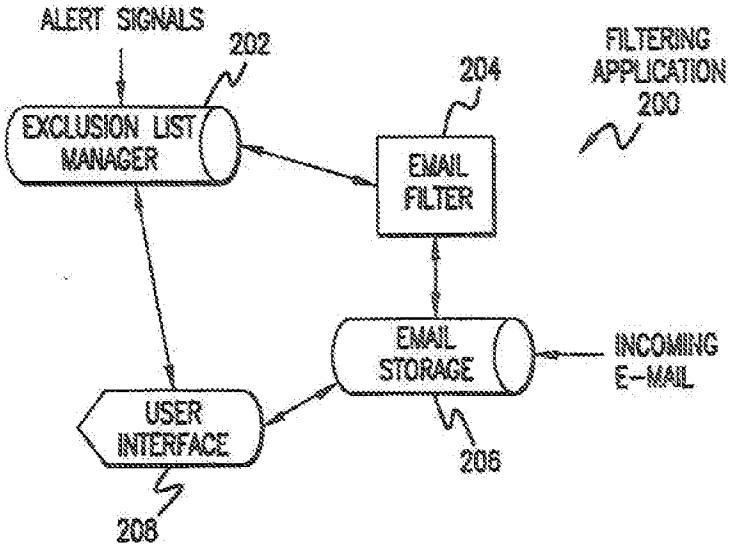
Published

Without international search report and to be republished upon receipt of that report.

(54) Title: APPARATUS AND METHOD FOR CONTROLLING DELIVERY OF UNSOLICITED ELECTRONIC MAIL

(57) Abstract

In a system and method and system for controlling delivery of unsolicited electronic mail messages, one or more spam probe e-mail addresses are created and planted at various sites on the communications network in order to insure their inclusion on large-scale electronic junk mail ("spam") mailing lists. The mailboxes corresponding to the spam probe e-mail addresses are monitored for incoming mail by a spam control center. Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received spam e-mail to identify the source of the message, extracts the spam source data from the message, and generates an alert signal containing the spam source data. This alert signal is broadcast to all network servers and/or all user terminals within the communications network. A filtering system implemented at the servers and/or user terminals receives the alert signal, updates stored filtering data using the spam source data retrieved from the alert signal, and controls delivery of subsequently-received e-mail messages received from the identified spam source. The filtering system controls delivery of the unsolicited e-mail messages by discarding the messages without displaying them to the user, displaying the messages to the user with a "JUNK" or similar marker, or otherwise processing the spam mail as desired by the network provider and/or the network users. The filtering system may also filter e-mail messages sent by the user terminals.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

APPARATUS AND METHOD FOR CONTROLLING DELIVERY OF UNSOLICITED ELECTRONIC MAIL

FIELD OF THE INVENTION

The present invention relates to a method and system for controlling the delivery of unsolicited electronic mail messages over an electronic communications network such as the Internet.

BACKGROUND OF THE INVENTION

The rapid increase in the number of users of electronic mail and the low cost of distributing electronic messages, for example, via the Internet and other communications networks has made mass marketing via electronic mail ("e-mail") an attractive advertising medium. Consequently, e-mail is now frequently used as the medium for widespread marketing broadcasts of unsolicited messages to e-mail addresses, commonly known as "spam."

Electronic mass marketers (also called "spammers") use a variety of techniques for obtaining e-mail address lists. For example, marketers obtain e-mail addresses from postings on various Internet sites such as news group sites, chat room sites, or directory services sites, message board sites, mailing lists, and by identifying "mailto" address links provided on web pages. Using these and other similar methods, electronic mass marketers may effectively obtain large numbers of mailing addresses, which become targets for their advertisements and other unsolicited messages.

Users of Internet services and electronic mail, however, are not eager to have their e-mail boxes filled with unsolicited e-mails. This is an increasing problem for Internet service providers (ISPs) such as America Online (AOL®) or Microsoft Network (MSN®) and other entities with easily identifiable e-mail addresses such as large corporations (e.g., IBM®, Microsoft®, General Motors®, etc.). ISPs object to junk mail because it reduces their users' satisfaction of their services. Corporations want to eliminate junk mail because it reduces worker productivity.

Accordingly, there is a need for a system that automatically and efficiently identifies unsolicited e-mails messages and controls the delivery of these messages to users, for example by preventing delivery of the messages to the users' in-boxes,

identifying the messages as unsolicited messages by displaying the messages in a distinctive display mode, or otherwise controlling the delivery of such messages to the users.

SUMMARY OF THE INVENTION

Accordingly, it is the object of the present invention to provide a system and method for controlling the delivery of unsolicited electronic mail messages ("spam") over an electronic communications network such as the Internet by identifying the source of identified spam transmissions using "spam probes," and automatically alerting network servers and/or user terminals to sources of spam in order to activate an effective filter or "spam wall" program implemented at network servers or user terminals or both.

According to the method and system of the present invention, one or more spam probe e-mail addresses are created and planted at various sites on the communications network in order to insure their inclusion on large-scale electronic junk mail ("spam") mailing lists. The mailboxes corresponding to the spam probe e-mail addresses are monitored for incoming mail by a spam control center. Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received mail to identify the source of the message, extracts and processes the source data from the received message, and generates an alert signal containing the processed source data. The alert signal may also contain filtering instructions used to enable network servers and user terminals to automatically detect spam. This alert signal is broadcast to all network servers or all user terminals, or both, within the communications network. A filtering system implemented at the servers or user terminals automatically receives the alert signal, automatically updates stored filtering data using the source data retrieved from the alert signal, and automatically controls delivery of subsequently-received e-mail messages from the identified spam source. Any filtering instructions are also stored and used to process incoming e-mail messages. The filtering system controls delivery of the unsolicited e-mail messages by discarding the messages without displaying them to the user, displaying the messages to the user with a "JUNK" or similar marker, or by otherwise processing the spam mail as desired by the network provider or the network users. The filtering system may also be used to filter e-mail messages sent from the user terminals.

A system for controlling delivery of unsolicited electronic mail according to the present invention includes a communications network including at least one user terminal and a control center. The control center includes a distributor for distributing a probe address to multiple sites on the communications network likely to be accessed by mailers of unsolicited electronic mail, a processor for receiving electronic mail messages addressed to the probe address and extracting source data from the received electronic mail messages, and an alert signal generator coupled to the processor for generating and transmitting an alert signal incorporating the extracted source data and, optionally, filtering instructions. The system according to the present invention may further include at least one network server coupled to the communications network and a plurality of user terminals coupled to the network server. A filtering application may be implemented in each of the network servers, each of the user terminals, or both. The filtering application receives the alert signal, updates stored filtering data upon receipt of the alert signal using the source data and filtering instructions retrieved from the alert signal, and filters electronic mail messages addressed to each of the user terminals in accordance with updated filtering data. The filtering system may also be used to filter e-mail messages sent from the user terminals.

A method of identifying sources of unsolicited electronic mail according to the present invention includes the steps of:

(a) creating a probe address; distributing the probe address to multiple sites on a communications network likely to be accessed by mailers of unsolicited electronic mail;

(b) monitoring the communications network for electronic mail addressed to the probe address;

(c) upon receipt of an electronic mail message addressed to the probe address, extracting and processing source data from the received electronic mail message; and

(d) generating an alert signal incorporating the processed source data.

A method for controlling delivery of unsolicited electronic mail according to the present invention includes the steps of:

(a) creating a probe address; distributing the probe address to multiple sites on a communications network likely to be accessed by mailers of unsolicited electronic mail;

(b) upon receipt of an electronic mail message addressed to the probe address, extracting and processing source data from the received electronic mail message;

(c) transmitting an alert signal incorporating the processed source data and, optionally, filtering instructions;

(d) receiving the alert signal at a filtering application for filtering electronic mail messages; updating filtering data stored by the filtering application using the source data and filtering instructions retrieved from the alert signal; and

(e) filtering the electronic mail messages received by the filtering application in accordance with the updated filtering data.

The foregoing and other features, aspects, and advantages of the present invention will become more apparent from the following detailed description when read in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 provides a block diagram of a system for controlling delivery of unsolicited electronic mail according to the present invention.

FIG. 2 provides a block diagram of user terminal-based filtering application for use in the system of FIG. 1.

FIG. 3 provides an example of data stored in an exclusion list used by the filtering application of FIG. 2.

FIG. 4 provides a block diagram of an alternative embodiment of a user terminal-based filtering application for use in the system of FIG. 1.

FIG. 5 provides a block diagram of network server-based filtering application for use in the system of FIG. 1

FIG. 6 provides a block diagram of an alternative embodiment of a network server-based filtering application for use in the system of FIG. 1

FIG. 7 provides a process flow chart for a method for identifying sources of unsolicited e-mail messages according to the present invention.

FIG. 8 provides a process flow chart for a method for controlling delivery of unsolicited e-mail messages according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described with reference to the accompanying drawings, which are provided as illustrative examples of preferred embodiments of the present invention. Notably, the present invention may be implemented using software, hardware or any combination thereof as would be apparent to one of skill in the art.

FIG. 1 depicts a preferred embodiment of a system 100 for controlling the delivery of unsolicited electronic mail messages. With reference to FIG. 1, a system 100 for controlling delivery of unsolicited electronic mail messages, e.g., spam, according to the present invention includes a control center 101 coupled to a communications network 110, for example, the Internet or other wide area network (WAN). A plurality of network servers 120, 121, and 122 are coupled to the control center 101 and the communications network 110. User terminals 130-138 are respectively coupled to servers 120-122 as shown in FIG. 1.

The control center 101 includes a processor 102 for creating spam probe addresses, a distributor 103 coupled to processor 102 for distributing the spam probe e-mail addresses to various sites within the communications network 110; a processor 104 coupled to the communications network 110 and distributor 103 for receiving e-mail addressed to the spam probe address and extracting and processing source data from the received e-mail messages addressed to the spam probe address; and an alert signal generator 105 coupled to processor 104 for generating alert signals to the servers 120-122 or user terminals 130-138, or both. The alert signals incorporate the source data from the e-mail messages addressed to the spam probe address extracted by processor 104 and may also incorporate filtering instructions entered, for example, via control terminal 106. Control terminal 106 is coupled to the control center 101 to control and monitor operation of the control center 101. Additional control terminals (not shown) may optionally be provided. The components of the control center 101 need not be consolidated in the same location and may be implemented as a distributed system of processors, components of a single processing system, or in other configurations as would be apparent to one of skill in the art.

Operation of the preferred embodiment of FIG. 1 will now be described in further detail. The system 100 for controlling delivery of unsolicited electronic mail messages according to the present invention as shown in FIG. 1 uses one or more "spam probes" created by processor 102 to identify sources of unsolicited e-mail or spam. A spam probe is an e-mail address specifically selected to make its way onto as many spammer mailing lists as possible. The spam probe is also selected to appear high up on the spammers' lists in order to receive mailings relatively early in the spammers' mailing process. For example, the spam probe address may be selected to appear at the top of an alphabetized mailing list (e.g., "Aardvark @aol.com"). In a preferred embodiment of the system according to the present invention, a certain percentage of assignable e-mail addresses offered by an ISP or private network are reserved for use as spam probes.

Once a spam probe is created using processor 102, distributor 103 distributes the spam probe to a number of sites on the communications network 110 likely to be browsed by spammers. For example, on the Internet, sites likely to be browsed by spammers may include chat room sites, directory services sites, mailing lists, message board sites, and news group sites as well as "mailto:" address links provided on posted web pages. In this way, the spam probe address preferably would be distributed to various locations on the network and posted with the intention that spammers will find the address and add to their mailing list as they browse the network.

After the spam probe has been distributed on the network 110, processor 104 stores the spam probe address received from distributor 103 and monitors the network 110 for e-mail messages addressed to the spam probe address. According to a preferred embodiment of the present invention, the mailbox corresponding to the spam probe address is located within processor 104. In this embodiment, all e-mail messages addressed to the spam probe address are automatically forwarded to processor 104 by the network 110.

In addition to receiving incoming e-mail messages automatically forwarded by the network 110, processor 104 may also use polling techniques known in the art to retrieve e-mail messages from probe address mailboxes by transmitting outgoing requests to the spam probe mailbox. Use of such methods helps to insure both timeliness of receipt of spam and immunity to denial of service attacks (for example, wherein a spammer sends

numerous processing commands to the spam probe server in order to keep the server busy, thereby preventing the server from receiving incoming e-mail messages).

Once the information contained in the received e-mail message is identified and received by processor 104, processor 104 analyzes this information using processing methods known in the art and extracts the source header data from the received e-mail message. In another preferred embodiment, a human operator may also perform additional analysis of the received e-mail messages using control terminal 106. Processor 104 then outputs the extracted source data to alert signal generator 105.

The processing performed by processor 104 may include analysis of the source header data from the received e-mail message in order to determine, for example, the Internet Protocol (IP) address of the sender or the address of the server(s) relaying the e-mail message from the sender to the spam probe mailbox using known look-up techniques. Processor 104 may also extract and analyze data from other fields of the received e-mail message, including other header fields such as the SUBJECT or MESSAGE ID fields, and the body of the e-mail message. Processor 104 provides the analyzed data to the alert signal generator 105.

Upon receipt of the data output from processor 104, alert signal generator 105 preferably generates an alert signal incorporating the source data extracted from the received e-mail message as well as other data analyzed by processor 104 (as described above). The alert signal may also incorporate filtering instructions to be implemented by the user terminals or network servers. Filtering instructions may be provided to the alert signal generator 105, for example, via control terminal 106. Alert signal generator 105 preferably then transmits the alert signal to each server 120-122 either via an optional dedicated communication link 140 or via the communications network 110.

Filtering instructions may be transmitted from the control center to the servers or user terminals or both to update and control the filtering operation performed by the servers or user terminals or both. For example, a filtering instruction may instruct the server or user terminal to compare the domain of the MESSAGE ID with the earliest source in the series of servers listed in the received field. If the domains of the two fields do not match, the server or user terminal would mark the e-mail message with a code, such as JUNK, indicating its status as spam. Other appropriate filtering instructions as

would be apparent to one of skill in the art may also be provided in order to insure effective spam filtering.

The system for controlling delivery of unsolicited e-mail shown in FIG. 1 includes a user terminal-based filtering application or a server-based filtering application, or a combination thereof. According to a preferred embodiment of the present invention, filtering applications implemented in the servers or user terminals are implemented using hardware or software, or a combination thereof, as is known in the art. The filtering applications receive and process the alert signals transmitted by alert signal generator 105 of the control center 101. Upon receipt of the alert signal, the filtering application (whether located in the servers or user terminals) extracts the source and other data (including filtering instructions, if any) from the alert signal. The filtering application stores the data and uses it to update its filtering process as described in further detail below with reference to FIGS. 2 through 6.

In the preferred embodiment depicted in FIG. 2, a user-terminal filtering application 200 for use in the present invention includes an exclusion list manager 202 for creating, storing and automatically maintaining a user exclusion list. The user exclusion lists preferably includes all identification data needed to determine the status of incoming e-mail messages. Data in the exclusion list may be divided into categories corresponding to the fields of incoming e-mail messages as illustrated in FIG. 3. For example, filtering using the "FROM" category of the exclusion list may be sufficient to control delivery of spam messages. However, users and/or service providers may optionally implement filtering based upon additional exclusion list categories, such as the "TO", "BCC," "CC," and "SUBJECT" e-mail headers and other headers. Fltering may also be based on the contents in the body of the email. The user exclusion list may be automatically created and maintained and/or created and modified manually by the user or service provider. The user terminal may also perform filtering based upon filtering instructions received from the control center 101.

In the preferred embodiment depicted in FIG. 4, alert signals received from the control center 101 are automatically processed by the filtering application so that the source data extracted from the alert signals are automatically added to the stored exclusion list. Thus, source data detected by the spam probe, processed by the control

center 101, and transmitted in the alert signals are used to automatically update the filtering applications in the user terminals 130-138.

The user terminal filtering application in the preferred embodiment depicted in FIG. 2 further includes an e-mail storage database 206, which receives and stores incoming e-mail and stores records of outgoing e-mail. An e-mail filter 204 filters the incoming e-mail stored in store 206 in accordance with the user exclusion list stored in database 202. A user interface 208 is provided to receive inputs from the user and to display e-mail information to the user. The user interface 208 may be implemented, for example, using an e-mail software package known in the art, such as Netscape® Messager®, Microsoft® Outlook®, Microsoft® Exchange®, Lotus® cc: mail®, Lotus Notes®, Novell® Groupwise®, Eudora®, or America OnLine®. User interface 208 may be used to display a user's mailbox, receive and process e-mail messages and inputs from the user, manage the user's mailbox, display mailbox management information to enable the user to manage the mailbox, and perform other functions as are known in the art.

Filtering of incoming e-mails may preferably be performed as follows. If the data in any of the "FROM" field of the incoming e-mail message match data stored in the corresponding data category of the exclusion list manager 202, the e-mail is marked by the filter 204 with a first display code indicating the "JUNK" status of the message. Optionally, the filter 204 may use multiple display codes indicating multiple status levels of "JUNK." If no match is detected between the fields of the received e-mail message and the stored exclusion list, the e-mail is marked with a second display code indicating the "OK" status of the message. Notably, the filtering system may be programmed to search not only for precise text in matching data fields, but also for similar text using known text searching techniques.

The marking of the incoming e-mail may be accomplished using known programming techniques, for example, by adding an additional field of information to the received e-mail format or by altering one or more existing e-mail fields to indicate the display status of the e-mail.

In one embodiment of the filtering application for use in the present invention, messages marked with the first display code indicating the "JUNK" status of the message are not displayed in the user's in-box and are automatically discarded by the filter.

Alternatively, the "JUNK" messages may be modified to indicate to the user that the messages are unsolicited, for example, by automatically inserting the word "JUNK" at the beginning of the message's "SUBJECT" header field, by displaying the message in a distinctive color in the user's in-box, by inserting the messages in a special folder in the user's in-box, or by other suitable means. Messages marked with the second display code indicating the "OK" status of the message preferably are automatically displayed in the user's inbox by the user interface 108 in a display mode visually distinct from the display mode for any displayed "JUNK" messages. Various known display methods may be used to distinguish "OK" mail messages from "JUNK" mail messages on the user's display screen.

In another preferred embodiment of the filtering system according to the present invention, e-mail messages marked with the first display code ("JUNK" mail) are further processed by the filter using user preference data entered by the user. The user may, for example, desire to receive unsolicited e-mail messages relating only to one or more specific subjects. Accordingly, the user may enter into his or her terminal a list of subjects which is stored as preference data by the filtering application. The filter application compares the subject data of the received e-mail message with subject preference data entered by the user. Notably, the subject data from the received message may include "SUBJECT" header information, the full text of the e-mail message, or both. A text search may be performed to determine whether the subject data from the received e-mail contains any of the subject words or phrases entered by the user as preference data. If a match is detected, the e-mail message is marked with a third display code and displayed to the user in a third distinctive mode using known display techniques. These e-mail messages may, for example, be automatically placed in a special folder created by the user or the filtering application or displayed in a distinctive color.

In yet another preferred embodiment of a filtering application for use in the present invention, the filtering application stores predetermined classification data, which are used to sort incoming unsolicited e-mail messages into predetermined categories. The filtering application may, for example, search the "SUBJECT" header data of the received e-mail message, other headers, the text of the message, or all three, to determine whether the subject data from the received message contain any words or phrases matching the subject information describing each predetermined category. In this

embodiment, each predetermined subject category of messages is associated with a specific display code. Accordingly, received messages in each predetermined category would be displayed to the user in different display modes to visually distinguish the categories on the user's display screen. The user may select to receive unsolicited e-mail messages in one or more of the predetermined categories, or none of the categories.

A filtering system according to the present invention may be implemented at the user terminal either as an integrated function within a user's e-mail program, such as Netscape Messager, Microsoft Outlook, Microsoft Exchange, Lotus cc: mail, Lotus Notes, Novell mail, Eudora, or AOL, or as a separate application that interacts with the user's existing e-mail application. In either embodiment, the e-mail filter 204 interacts with the e-mail store 206 to access, modify, and categorize e-mail messages as described above. The filtering system may also be used to filter outgoing e-mail messages sent by the user terminals.

FIG. 4 illustrates an alternative embodiment in which the filtering application is implemented, for example, at the user terminal 130 shown in FIG. 1. The e-mail filter 204 receives and filters incoming e-mail messages before they are stored in e-mail store 206, and may also filter outgoing messages sent by the user terminals. This embodiment may be implemented using a known message communications means, such as Microsoft's Mail API (MAPI) or an Internet mail protocol such as Post Office Protocol (POP3), IMAP or Simple Mail Transfer Protocol (SMTP). In a preferred embodiment using user terminal filtering, the system according to the present invention may be implemented as an add-on system to a known e-mail software package using MAPI configured as a network service provider. This embodiment has the advantage of simplifying the implementation of the present invention at the user terminal.

FIG. 5 illustrates preferred a server-side embodiment in which the present invention is implemented within network servers. This embodiment enables filtering to be performed at a relatively small number of locations for all users within a network. A server, e.g., 120 shown in FIG. 1, receives and routes e-mail messages to and from a plurality of user terminals 130-133 shown in FIG. 1. The server 120 includes an e-mail server message store 506 for receiving and storing all e-mail messages transmitted within the network 110 and an e-mail filter 504. An exclusion list processor 502 stores and maintains at least one exclusion list for each e-mail address that is serviced by the e-mail

server 120. For example, in the network configuration of FIG. 5, the exclusion list processor 502 maintains a separate user exclusion list for each user terminal, for example, user terminals 130-133 shown in FIG. 1. The server 120 may also filter outbound messages sent by the users using a similar filtering operation.

An additional functionality of the present invention that may be implemented within the above-described preferred embodiment or separately implemented in a different embodiment of the present invention is a functionality by which multiple exclusion lists are maintained. One or more selected exclusion lists are applied in filtering for all user terminals 130-133. One or more selected exclusion lists are applied in filtering for only certain user terminals, e.g., only user terminal 130. Accordingly, this embodiment of the present invention offers selective filtering of certain user terminals and general filtering of all user terminals.

The operation of the components of the server 120 shown in FIG. 5 is similar to the corresponding components in the user-site system of FIG. 2. All e-mail received by server 120 is stored in e-mail store 506. The e-mail filter 504 filters the stored e-mail messages in accordance with the information stored in the exclusion list processor 502. E-mail addressed to each user terminal 130-133 shown in FIG. 1 is separately filtered using the exclusion list stored for each user respectively. Once the e-mail stored in store 506 is processed by e-mail filter 504, the filtered e-mail is then forwarded to the users' respective user sites.

The filtering process performed for each user terminal, e.g., 130, by the e-mail filter 504 is the same as that performed by filter 204 in FIG. 2. The filter 504 compares the data stored in the "FROM" header field (and optionally the "TO," "CC," "BCC," and "SUBJECT" fields and associated sub-headers fields) of the incoming e-mail messages with corresponding categories of data stored in the exclusion list processor 502. If data in any of these fields of the incoming e-mail matches data stored in a corresponding field of the inclusion list processor 502, the incoming e-mail is marked "JUNK" and marked with a first display code. If no match is detected, the e-mail filter labels the e-mail message as "JUNK" by marking the message with a second display code. Further processing to display the JUNK messages by subjects or subject categories as described above with reference to FIG. 5 may also be performed by the server's filtering application.

In the preferred server-side embodiment shown in FIG. 5, the e-mail filter 504 interacts with the e-mail message store 506 that processes the e-mail and performs other known functions for a multiplicity of e-mail addresses or accounts. In this embodiment, the e-mail store 506 may store additional information about the category of each e-mail message. In an alternative preferred embodiment, the status of e-mail messages is handled in a separate database (not shown) outside the message store 506.

The exclusion list processor 502 may store an exclusion list for each e-mail address or, alternatively, an exclusion list for each group of e-mail addresses organized by domain or other group. According to another preferred embodiment, each exclusion list created and maintained by the exclusion list processor 502 includes an additional data field to identify characteristics of at least one user account or e-mail address. This embodiment has the advantage of providing centralized management of account information.

FIG. 6 illustrates an alternative preferred embodiment in which the e-mail filter receives and filters incoming e-mail messages before they are stored in e-mail store 506. This embodiment may be implemented using a known message communications means, such as MAPI or an Internet mail protocol such as POP3, IMAP or SMTP. This embodiment has the advantage of reducing the data traffic flow on a communications link by filtering out junk e-mail before it is stored at the server.

The preferred embodiment of a server-based filtering application has the advantage of enabling quick deployment of the invention because server software can generally be updated more quickly than user terminal software. Filtering rules may be updated in real-time or near real-time on the server, allowing rapid response to new instances of junk mail. This embodiment also has the advantage of ease of implementation in an environment where there are multiple e-mail users. This embodiment also has the potential advantage of reducing the wasted bandwidth of sending junk e-mail messages to users who will not read them.

Additional control of the filtering applications implemented at the user terminals or servers, or both, may optionally be provided via the control terminal 106 shown in FIG. 1 and/or a control terminal (not shown) coupled to one or more of servers 120-122. Using these control terminals, a system operator may enter source data or subject data, or both, to be added to the filtering application exclusion lists. Accordingly, a service

provider may prevent users from receiving e-mails from specific sources or e-mail messages including certain subject matter (e.g., pornographic subject matter) by adding source data and/or subject data to the filtering application exclusion lists. The network users may or may not be given authorization to access or change the exclusion list data entered by the system operator. Service provider entries in the exclusion list may or may not be displayed to the users.

Users may manually implement similar limitations for their mailboxes by manually entering data into the exclusion list.

With reference to FIG. 7, a method for identifying sources of unsolicited electronic mail according to the present invention includes the following steps:

701 - creating a spam probe address;

702 - distributing the spam probe address to multiple sites on a communications network likely to be accessed by mailers of unsolicited electronic mail;

703 - upon receipt of an electronic mail message addressed to the spam probe address, extracting source data from the received electronic mail message; and

704 - generating an alert signal incorporating the extracted source data.

With reference to FIG. 8, a method of controlling delivery of unsolicited electronic mail messages according to the present invention includes the following steps:

801 - creating a spam probe address;

802 - distributing the spam probe address to multiple sites on a communications network likely to be accessed by mailers of unsolicited electronic mail;

803 - upon receipt of an electronic mail message addressed to the spam probe address, extracting source data from the received electronic mail message;

804 - transmitting an alert signal incorporating the extracted source data;

805 - receiving the alert signal at a filtering application for filtering electronic mail messages;

806 - updating filtering data stored by the filtering application using the source data retrieved from the alert signal; and

807 - filtering the electronic mail messages received by the filtering application in accordance with the updated filtering data.

The filtering method according to the present invention may also be implemented in combination with one or more inclusion-based filtering methods as would be apparent to one of skill in the art.

While the present invention has been particularly described with reference to the preferred embodiments, it should be readily apparent to those of ordinary skill in the art that changes and modifications in form and details may be made without departing from the spirit and scope of the invention. It is intended that the appended claims include such changes and modifications.

CLAIMS

I claim:

1. A system for controlling delivery of unsolicited electronic mail, comprising:

a communications network;

a control center, comprising

a distributor for distributing a probe address to at least one site on said communications network,

a processor for receiving electronic mail messages addressed to said probe address, and for extracting source data from said received electronic mail message, and

an alert signal generator coupled to said processor for generating and transmitting an alert signal incorporating said extracted source data; and

a plurality of user terminals coupled to said communications network, each comprising a filtering application for receiving said alert signal, updating stored filtering data upon receipt of said alert signal, and filtering electronic mail messages received by said user terminal in accordance with said updated filtering data.

2. A system according to claim 1, wherein said user terminals filter electronic mail messages sent from said user terminals in accordance with said updated filtering data.

3. A system for controlling delivery of unsolicited electronic mail, comprising:

a communications network;

a control center, comprising

a distributor for distributing a probe address to at least one site on said communications network,

a processor for receiving electronic mail messages addressed to said probe address, and for extracting source data from said received electronic mail message, and

an alert signal generator coupled to said processor for generating and transmitting an alert signal;

a server coupled to said communications network; and

a plurality of user terminals coupled to said server,

wherein said server comprises a filtering application for receiving said alert signal, updating stored filtering data upon receipt of said alert signal, and filtering electronic mail messages addressed to each of said plurality of user terminals in accordance with said updated filtering data.

4. A system according to claim 3, wherein said alert signal incorporates said extracted source data.

5. A system according to claim 3, wherein said server also filters electronic mail messages sent from each of said plurality of user terminals.

6. A method of identifying sources of unsolicited electronic mail, comprising the steps of:

creating a probe address;

distributing said probe address to multiple sites on a communications network;

upon receipt of an electronic mail message addressed to said probe address, extracting source data from said received electronic mail message; and

generating an alert signal incorporating said extracted source data.

7. A method for controlling delivery of unsolicited electronic mail, comprising the steps of:

creating a probe address;

distributing said probe address to multiple sites on a communications network;

upon receipt of an electronic mail message addressed to said probe address, extracting source data from said received electronic mail message;

transmitting an alert signal incorporating said extracted source data;

receiving said alert signal at a filtering application for filtering electronic mail messages;

updating filtering data stored by said filtering application; and

filtering said electronic mail messages received by said filtering application in accordance with said updated filtering data.

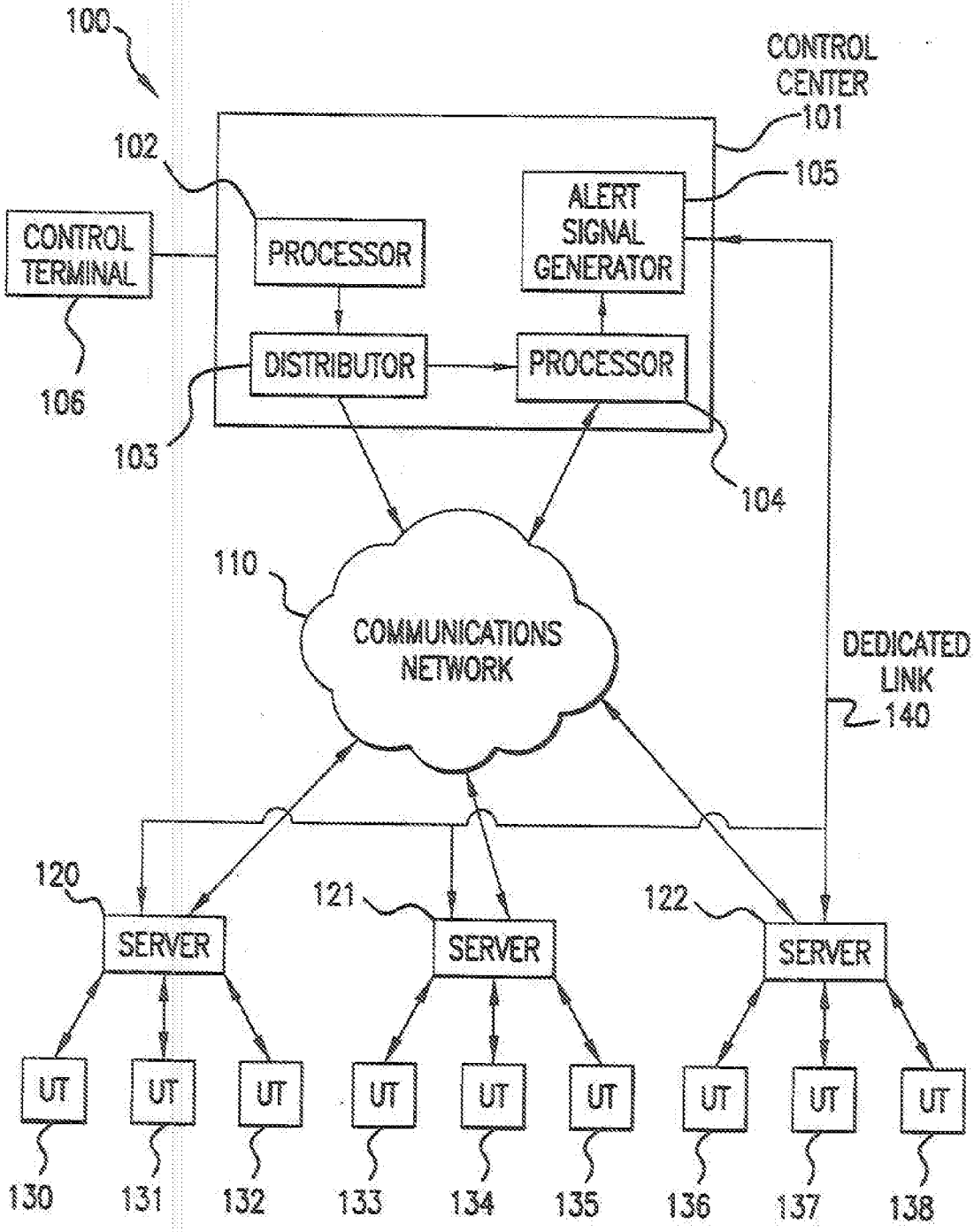

100
CONTROL CENTER
101
102
105
CONTROL TERMINAL
PROCESSOR
ALERT SIGNAL GENERATOR
DISTRIBUTOR
PROCESSOR
106
103
104
110
COMMUNICATIONS NETWORK
DEDICATED LINK
140
120
121
122
SERVER
SERVER
SERVER
UT
UT
UT
UT
UT
UT
UT
UT
UT
130
131
132
133
134
135
136
137
138

FIG. 1

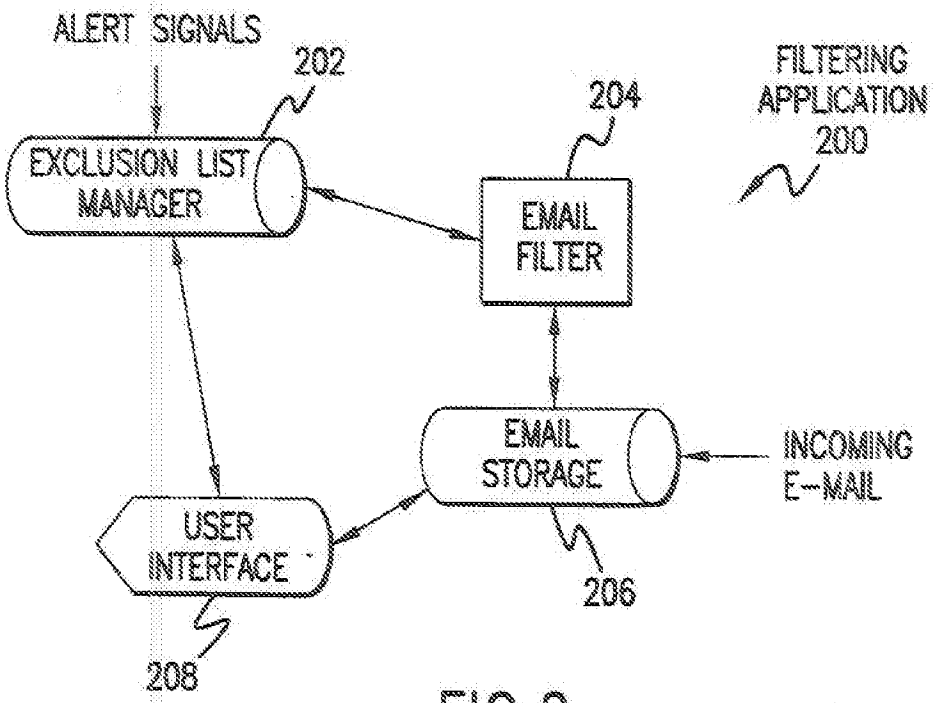


FIG.2

"FROM"	"TO"	"CC"	"BCC"	"SUBJECT"
SPAM.COM	MASSMAILING	MASSMAILING	MASSMAILING	SOLICITATION
ADVERTISER.COM				CREDIT CARD OFFER
MASSMARKET.COM				
EXFIANCEE.COM				

FIG.3

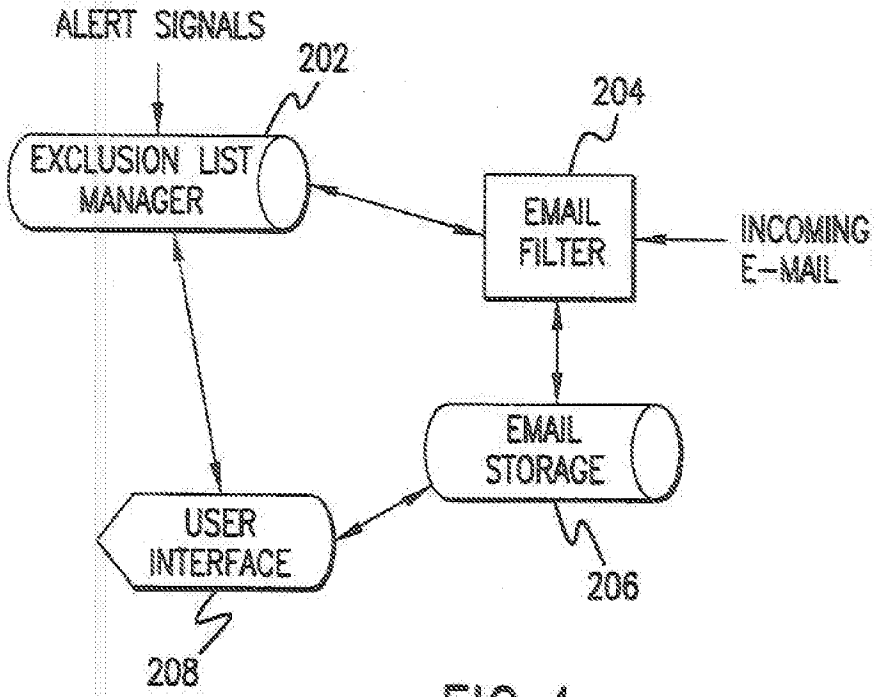

ALERT SIGNALS
202
204
EXCLUSION LIST MANAGER
EMAIL FILTER
INCOMING E-MAIL
EMAIL STORAGE
USER INTERFACE
206
208

FIG.4

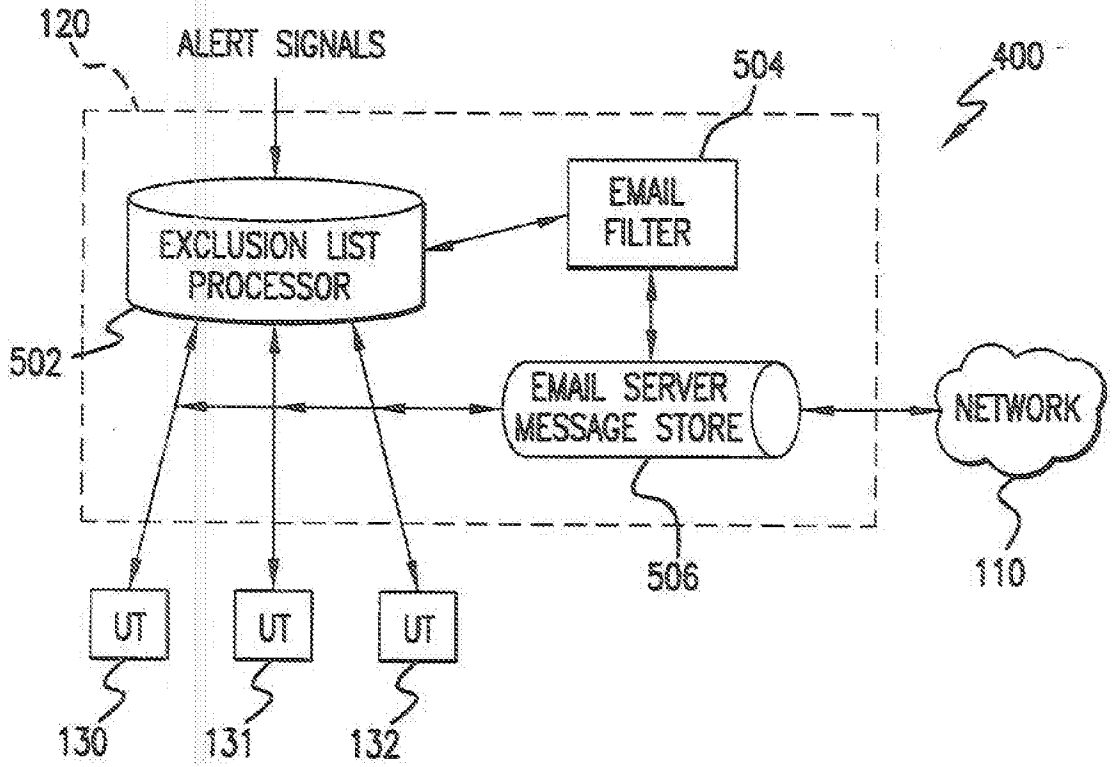
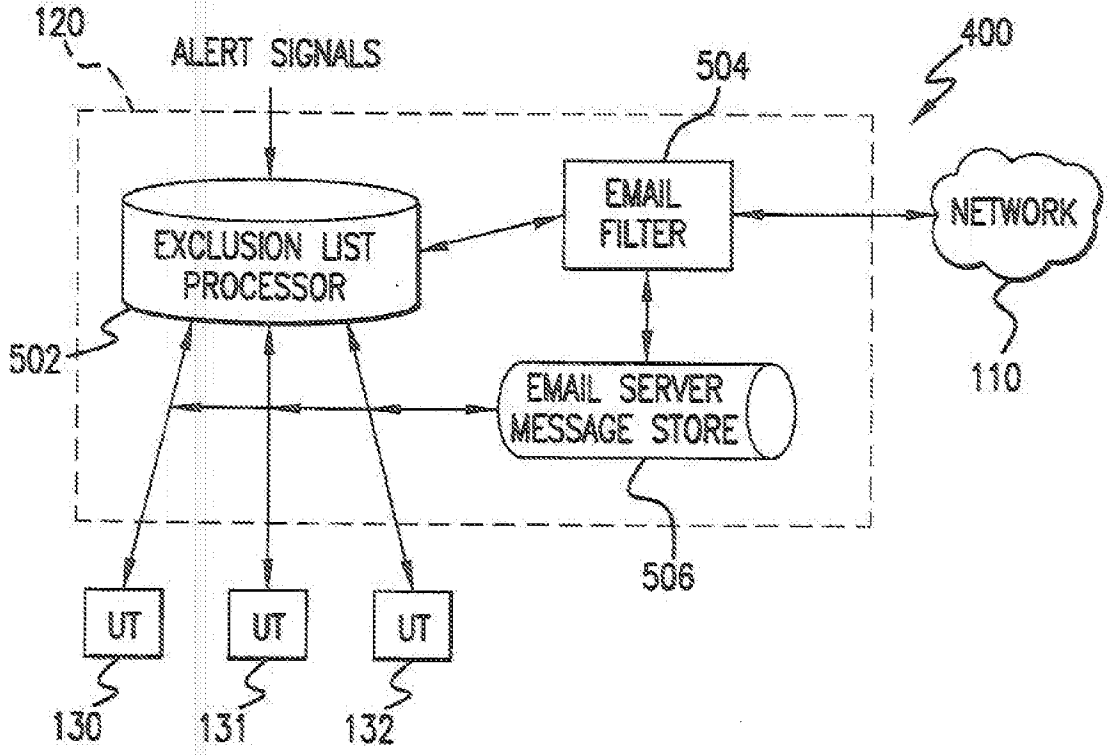

120
ALERT SIGNALS
504
400
EMAIL FILTER
EXCLUSION LIST PROCESSOR
502
EMAIL SERVER MESSAGE STORE
NETWORK
506
110
UT
UT
UT
130
131
132

FIG.5


120
ALERT SIGNALS
504
400
EMAIL FILTER
NETWORK
EXCLUSION LIST PROCESSOR
502
110
EMAIL SERVER MESSAGE STORE
506
UT
UT
UT
130
131
132

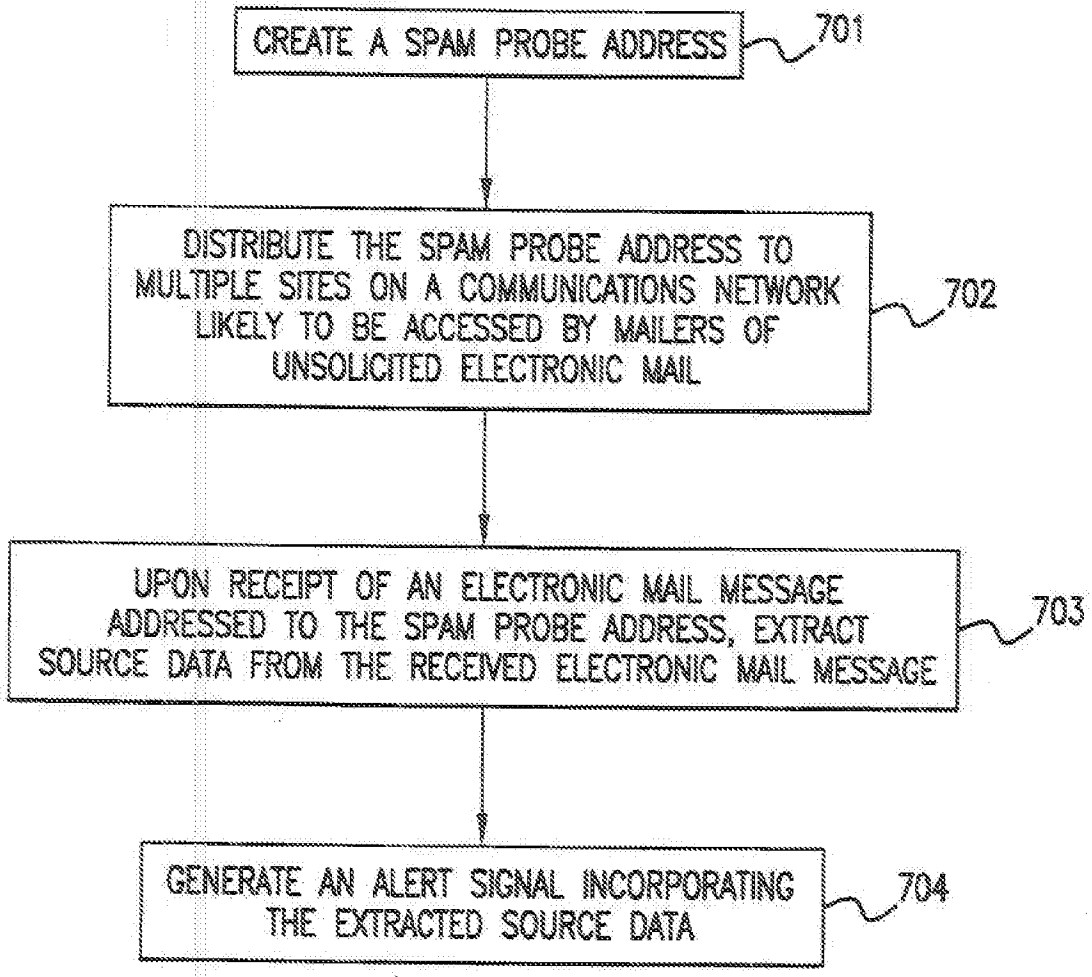

CREATE A SPAM PROBE ADDRESS
701
DISTRIBUTE THE SPAM PROBE ADDRESS TO MULTIPLE SITES ON A COMMUNICATIONS NETWORK LIKELY TO BE ACCESSED BY MAILERS OF UNSOLICITED ELECTRONIC MAIL
702
UPON RECEIPT OF AN ELECTRONIC MAIL MESSAGE ADDRESSED TO THE SPAM PROBE ADDRESS, EXTRACT SOURCE DATA FROM THE RECEIVED ELECTRONIC MAIL MESSAGE
703
GENERATE AN ALERT SIGNAL INCORPORATING THE EXTRACTED SOURCE DATA
704

FIG.7

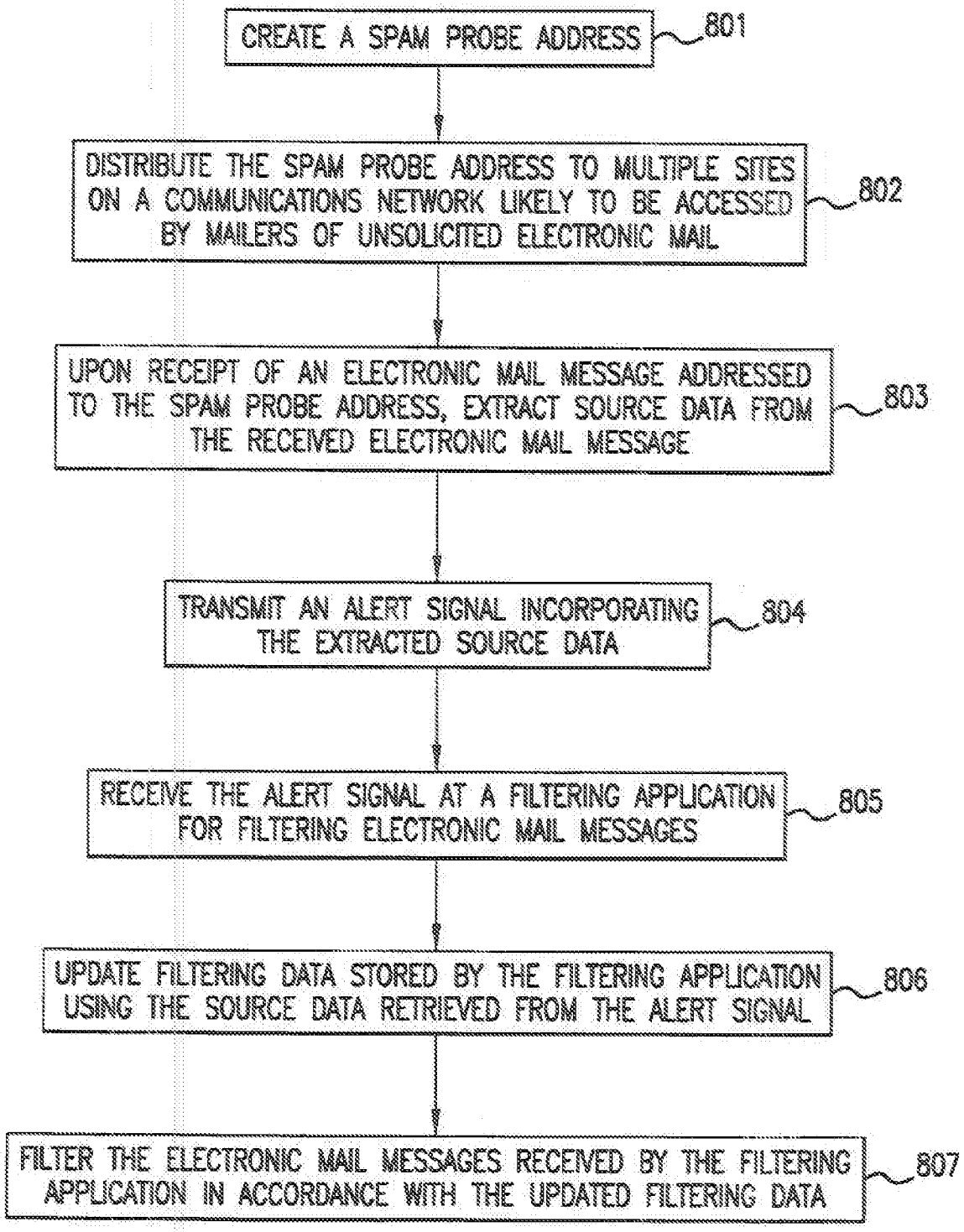

CREATE A SPAM PROBE ADDRESS
801
DISTRIBUTE THE SPAM PROBE ADDRESS TO MULTIPLE SITES ON A COMMUNICATIONS NETWORK LIKELY TO BE ACCESSED BY MAILERS OF UNSOLICITED ELECTRONIC MAIL
802
UPON RECEIPT OF AN ELECTRONIC MAIL MESSAGE ADDRESSED TO THE SPAM PROBE ADDRESS, EXTRACT SOURCE DATA FROM THE RECEIVED ELECTRONIC MAIL MESSAGE
803
TRANSMIT AN ALERT SIGNAL INCORPORATING THE EXTRACTED SOURCE DATA
804
RECEIVE THE ALERT SIGNAL AT A FILTERING APPLICATION FOR FILTERING ELECTRONIC MAIL MESSAGES
805
UPDATE FILTERING DATA STORED BY THE FILTERING APPLICATION USING THE SOURCE DATA RETRIEVED FROM THE ALERT SIGNAL
806
FILTER THE ELECTRONIC MAIL MESSAGES RECEIVED BY THE FILTERING APPLICATION IN ACCORDANCE WITH THE UPDATED FILTERING DATA
807

FIG.8

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60 — A3

(11) International Publication Number: WO 99/33188

(43) International Publication Date: 1 July 1999 (01.07.99)

(21) International Application Number: PCT/US98/25961

(22) International Filing Date: 8 December 1998 (08.12.98)

(30) Priority Data:
08/997,692 23 December 1997 (23.12.97) US

(71) Applicant: BRIGHT LIGHT TECHNOLOGIES, INC. [US/US]; Suite 300, 651 Brannan Street, San Francisco, CA 94107 (US).

(72) Inventor: PAUL, Sunil; 1506 Willard Street, San Francisco, CA 94117 (US).

(74) Agent: LUEDKE, Adrienne, Suringa; Covington & Burling, 1201 Pennsylvania Avenue, N.W., P.O. Box 7566, Washington, DC 20044–7566 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

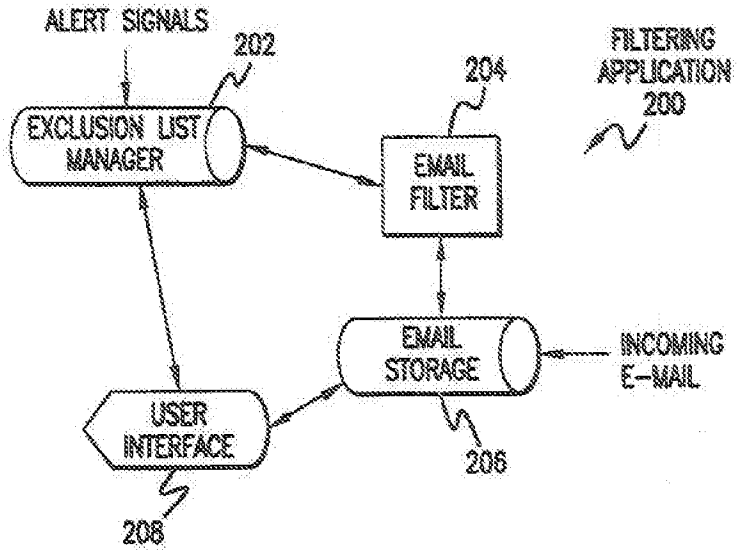
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
26 August 1999 (26.08.99)

(54) Title: APPARATUS AND METHOD FOR CONTROLLING DELIVERY OF UNSOLICITED ELECTRONIC MAIL

(57) Abstract

In a system and method and system for controlling delivery of unsolicited electronic mail messages, one or more spam probe e-mail addresses are created and planted at various sites on the communications network in order to insure their inclusion on large-scale electronic junk mail ("spam") mailing lists. The mailboxes corresponding to the spam probe e-mail addresses are monitored for incoming mail by a spam control center. Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received spam e-mail to identify the source of the message, extracts the spam source data from the message, and generates an alert signal containing the spam source data. This alert signal is broadcast to all network servers and/or all user terminals within the communications network. A filtering system implemented at the servers and/or user terminals receives the alert signal, updates stored filtering data using the spam source data retrieved from the alert signal, and controls delivery of subsequently-received e-mail messages received from the identified spam source. The filtering system controls delivery of the unsolicited e-mail messages by discarding the messages without displaying them to the user, displaying the messages to the user with a "JUNK" or similar marker, or otherwise processing the spam mail as desired by the network provider and/or the network users. The filtering system may also filter e-mail messages sent by the user terminals.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 98/25961

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RANUM M J ET AL: "Implementing a generalized tool for network monitoring" PROCEEDINGS OF THE ELEVENTH SYSTEMS ADMINISTRATION CONFERENCE (LISA XI), PROCEEDINGS OF THE ELEVENTH SYSTEMS ADMINISTRATION CONFERENCE (LISA XI), SAN DIEGO, CA, USA, 26-31 OCT. 1997, pages 1-8, XP002107361 ISBN 1-880446-90-1, 1997, Berkeley, CA, USA, USENIX Assoc, USA see page 2, column 1, paragraph 3 - page 3, column 2, paragraph 2 see page 5, column 1, paragraph 2 - page 7, column 2, paragraph 3 --- -/--	1-7

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 June 1999	12/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gardiner, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 98/25961

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELSVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	CRANOR L F ET AL: "SPAM" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, vol. 41, no. 8, 1 August 1998, pages 74-83, XP000789467 see page 78, column 1, paragraph 3 - page 80, column 2, paragraph 1 ---	1-7
A	LEFEBVRE W: "Sendmail and spam" UNIX REVIEW'S PERFORMANCE COMPUTING, AUG. 1998, MILLER FREEMAN, USA, vol. 16, no. 9, pages 55-58, XP002107362 ISSN 0742-3136 see the whole document -----	1-7

Form PCT/ISA/210 (continuation of second sheet) (July 1992)